

09/807824

PCT/JP00/05543

180800

日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 04 SEP 2000

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1999年 8月20日

出願番号

Application Number:

平成11年特許願第234371号

出願人

Applicant (s):

ソニー株式会社

EJV

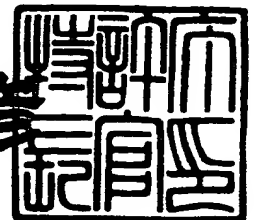
PRIORITY
DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 6月29日

特許庁長官
Commissioner,
Patent Office

近藤隆彦



出証番号 出証特2000-3049977

【書類名】 特許願

【整理番号】 9900417005

【提出日】 平成11年 8月20日

【あて先】 特許庁長官 殿

【国際特許分類】 G11B 7/00

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 浅野 智之

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 大澤 義知

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100067736

【弁理士】

【氏名又は名称】 小池 晃

【選任した代理人】

【識別番号】 100086335

【弁理士】

【氏名又は名称】 田村 榮一

【選任した代理人】

【識別番号】 100096677

【弁理士】

【氏名又は名称】 伊賀 誠司

【手数料の表示】

【予納台帳番号】 019530

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707387

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報記録／再生システム、情報記録／再生装置、情報記録／再生方法及び情報記録媒体

【特許請求の範囲】

【請求項 1】 セキュリティモジュールを有する情報記録媒体と、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体に記録、あるいは、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体から再生する情報記録／再生装置とを備え、

情報記録時、又は情報再生時に上記情報記録／再生装置とセキュリティモジュールとが公開鍵暗号技術を用いた相互認証プロトコルを実行することを特徴とする情報記録／再生システム。

【請求項 2】 上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報（ID）がリボケーションリストに掲載されていないことを確認することを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 3】 上記相互認証プロトコルの実行時に、上記記録／再生装置とセキュリティモジュールが、互いに、自分が所有するリボケーションリストのバージョンナンバーを教え合い、新しいリボケーションリストを持つものがそれを他方に送り、古いリボケーションリストを持つものは送られた新しいリボケーションリストを用いて自分のリボケーションリストを置き換えることを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 4】 データの記録時又は再生時に、上記情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを暗号化する暗号鍵を一方が暗号化して他方に送ることを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 5】 データの記録時又は再生時に、上記情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いてデータを一方が暗号化して他方に送ることを特徴とする請求項 1 記

載の情報記録／再生システム。

【請求項 6】 データを格納する情報記録媒体への書き込み、読み出しのアクセスは、上記セキュリティモジュールを介して行われることを特徴とする請求項 1 記載の情報記録／再生システム。

【請求項 7】 データの記録時に、上記情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いて鍵共有プロトコルを実行し、共有された鍵を用いて上記情報記録／再生装置がデータを暗号化してセキュリティモジュールに送り、上記セキュリティモジュールは、共有された鍵を用いてこれを復号して平文データを得た後に、暗号鍵を用いてデータを暗号化して情報記録媒体に格納することを特徴とする請求項 6 記載の情報記録／再生システム。

【請求項 8】 データの再生時に、上記セキュリティモジュールが暗号化されて情報記録媒体に格納されているデータを読み出し、暗号鍵を用いてこれを復号して平文データを得た後、上記情報記録／再生装置とセキュリティモジュールが鍵共有プロトコルを実行した結果共有された鍵を用いてデータを上記セキュリティモジュールが暗号化して情報記録／再生装置に送ることを特徴とする請求項 6 記載の情報記録／再生システム。

【請求項 9】 データの記録時及び再生時に、情報記録／再生装置との間で公開鍵暗号を用いた相互認証プロトコルを実行するセキュリティモジュールを有することを特徴とする情報記録媒体。

【請求項 10】 上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、情報記録／再生装置の識別情報（ID）がリボケーションリストに掲載されていないことを確認することを特徴とする請求項 9 記載の情報記録媒体。

【請求項 11】 上記セキュリティモジュールは、上記相互認証プロトコルを実行するときに、自分が持つリボケーションリストのバージョンナンバーを情報記録／再生装置に送り、これと上記情報記録／再生装置が送ったリボケーションリストのバージョンナンバーを受信して比較し、自分のものの方が新しい場合にはリボケーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたリボケーションリストを現在自分が持っているものと置き換える処

理を行うことを特徴とする請求項 9 記載の情報記録媒体。

【請求項 12】 上記セキュリティモジュールが管理する暗号鍵を用いて暗号化されたデータを格納することを特徴とする請求項 9 記載の情報記録媒体。

【請求項 13】 上記セキュリティモジュールは、データの記録時及び再生時に、情報記録／再生装置との間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて、データを暗号化する暗号鍵を情報記録／再生装置に送信あるいは情報記録／再生装置から受信することを特徴とする請求項 9 記載の情報記録媒体。

【請求項 14】 データの書き込み及び読み出しの処理が上記セキュリティモジュールを介して行われることを特徴とする請求項 9 記載の情報記録媒体。

~~【請求項 15】 上記セキュリティモジュールは、データの記録時に、情報記録／再生装置との間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて受信したデータを復号し、さらに別の鍵を用いてデータを暗号化することを特徴とする請求項 14 記載の情報記録媒体。~~

【請求項 16】 データの再生時に、記録媒体からデータを読み出して暗号鍵 1 を用いて復号した後、情報記録／再生装置との間で公開鍵暗号を用いた鍵共有プロトコルを実行し、共有した鍵を用いてデータを暗号化して情報記録／再生装置に送信することを特徴とする請求項 14 記載の情報記録媒体。

【請求項 17】 データの記録時及び再生時に、情報記録媒体のセキュリティモジュールとの間で公開鍵暗号を用いた相互認証プロトコルを実行する制御手段を備えることを特徴とする情報記録／再生装置。

【請求項 18】 上記制御手段は、上記相互認証プロトコルを実行するときに、上記セキュリティモジュールの識別情報 (ID) がリボケーションリストに掲載されていないことを確認することを特徴とする請求項 17 記載の情報記録／再生装置。

【請求項 19】 上記制御手段は、上記相互認証プロトコルを実行するときに、自分が持つリボケーションリストのバージョンナンバーをセキュリティモジュールに送り、これと上記セキュリティモジュールが送ったリボケーションリストのバージョンナンバーを受信して比較し、自分のものの方が新しい場合にはリボ

ケーションリストを相手に送り、相手のものの方が新しい場合には、相手から送られたリボケーションリストを現在自分が持っているものと置き換える処理を行うことを特徴とする請求項 1 7 記載の情報記録／再生装置。

【請求項 2 0】 上記制御手段は、データの記録時及び再生時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて、データを暗号化する暗号鍵を上記セキュリティモジュールに送信あるいは上記セキュリティモジュールから受信することを特徴とする請求項 1 7 記載の情報記録／再生装置。

【請求項 2 1】 上記制御手段は、データの記録時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いてデータを暗号化して情報記録媒体に格納することを特徴とする請求項 1 7 記載の情報記録／再生装置。

【請求項 2 2】 上記制御手段は、データの記録時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いてデータを暗号化して上記セキュリティモジュールに送信することを特徴とする請求項 1 7 記載の情報記録／再生装置。

【請求項 2 3】 上記制御手段は、データの記録時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いてデータの暗号化に用いる暗号鍵を暗号化して上記セキュリティモジュールに送信し、又は共有した鍵を用いて暗号化された暗号鍵を上記セキュリティモジュールから受信し、上記暗号鍵を用いてデータを暗号化して上記セキュリティモジュールに送信することを特徴とする請求項 1 7 記載の情報記録／再生装置。

【請求項 2 4】 上記制御手段は、データの再生時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有した鍵を用いて、上記セキュリティモジュールから送られたデータを復号することを特徴とする請求項 1 7 記載の情報記録／再生装置。

【請求項 2 5】 上記制御手段は、データの再生時に、上記セキュリティモジュールとの間で公開鍵暗号を用いた鍵共有プロトコルを実行し、この際に共有し

た鍵を用いて、データの暗号化に用いる暗号鍵を暗号化してセキュリティモジュールに送信し、又は共有した鍵を用いて暗号化された暗号鍵を上記セキュリティモジュールから受信し、上記暗号鍵を用いて上記セキュリティモジュールから送られたデータを復号することを特徴とする請求項 17 記載の情報記録／再生装置。

【請求項 26】 情報記録／再生装置により情報記録媒体にデータを記録、あるいは情報記録媒体からデータを再生する情報記録／再生方法において、

情報記録媒体が有するセキュリティモジュールと情報記録／再生装置が公開鍵暗号を用いた相互認証プロトコルを実行するステップを有することを特徴とする情報記録／再生方法。

【請求項 27】 上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、他方の識別情報（ID）がリボケーションリストに掲載されていないことを確認するステップを有することを特徴とする請求項 26 記載の情報記録／再生方法。

【請求項 28】 上記相互認証プロトコルを実行するときに、情報記録／再生装置とセキュリティモジュールが、互いに、自分が所有するリボケーションリストのバージョンナンバーを教えるステップと、新しいリボケーションリストを持つものがそれを他方に送るステップと、古いリボケーションリストを持つものは送られた新しいリボケーションリストを用いて自分のリボケーションリストを置き換えるステップを有することを特徴とする請求項 26 記載の情報記録／再生方法。

【請求項 29】 データの記録時又は再生時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを実行するステップと、共有された鍵を用いてデータを暗号化する暗号鍵を一方が暗号化して他方に送るステップを有することを特徴とする請求項 26 記載の情報記録／再生方法。

【請求項 30】 データの記録時又は再生時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを行うステップと、共有された鍵を用いてデータを一方が暗号化して他方に送るステップを有することを特徴とする請求項 26 記載の情報記録／再生方法。

【請求項 3 1】 データの記録時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを実行するステップと、共有された鍵を用いてデータを情報記録／再生装置が暗号化して他方に送るステップと、セキュリティモジュールが受信したデータを共有された鍵を用いて復号するステップと、セキュリティモジュールが上記復号したデータを鍵を用いて暗号化するステップと、セキュリティモジュールが上記暗号化したデータを情報記録媒体に格納するステップを有することを特徴とする請求項 2 6 記載の情報記録／再生方法。

【請求項 3 2】 データの再生時に、情報記録／再生装置とセキュリティモジュールが公開鍵暗号を用いた鍵共有プロトコルを行って鍵を共有するステップと

セキュリティモジュールが情報記録媒体からデータを読み出して鍵を用いて復号するステップと、セキュリティモジュールが上記復号後のデータを共有した鍵を用いて暗号化するステップと、セキュリティモジュールが上記暗号化後のデータを情報記録／再生装置に送信するステップとを有することを特徴とする請求項 2 6 記載の情報記録／再生方法。

【請求項 3 3】 外部装置とインタフェースをとるためのインタフェース機能と、乱数を生成するための乱数生成機能と、情報を保存するための記憶機能と、公開鍵暗号技術を用いた相互認証プロトコルに必要な計算を行う演算機能を有するセキュリティモジュールを備えることを特徴とする情報記録媒体。

【請求項 3 4】 上記セキュリティモジュールは、データを記録するための記録領域にアクセスするためのインタフェース機能を備えることを特徴とする請求項 3 3 記載の情報記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、安全にデータを授受することを可能にした情報記録／再生システム、情報記録装置及び情報再生装置等に関する。

【 0 0 0 2 】

【従来の技術】

近年、情報をデジタル的に記録する記録装置及び記録媒体が普及しつつある。これらの記録装置及び記録媒体は、例えば、映像や音楽のデータを劣化させることなく記録し、再生するので、データを、その質を維持しながら何度もコピーすることができる。しかしながら、映像や音楽のデータの著作権者にしてみれば、自らが著作権を有するデータが、その質を維持しながら何度も不正にコピーされ、市場に流通してしまう恐れがある。このため、記録装置及び記録媒体の側で、著作権を有するデータが不正にコピーされるのを防ぐ必要がある。

【 0 0 0 3 】

~~このような著作権保護のためのシステムとして、例えば、ミニディスク (MD)~~
(商標) システムにおいては、SCMS (Serial Copy Management System) と呼ばれる方法が用いられている。これは、デジタルインタフェースによって、音楽データとともに伝送される情報のことである。この情報は、音楽データが、copy free、copy once allowed、又はcopy prohibited のうちのいずれのデータであるのかを表す。ミニディスクレコーダは、デジタルインタフェースから音楽データを受信した場合、SCMSを検出し、これが、copy prohibited であれば、音楽データをミニディスクに記録せず、copy once allowedであれば、これをcopy prohibitedに変更し、受信した音楽データとともに記録し、copy freeであれば、これをそのまま、受信した音楽データとともに記録する。

【 0 0 0 4 】

このようにして、ミニディスクシステムにおいては、SCMSを用いて、著作権を有するデータが不正にコピーされるのを防いでいる。

【 0 0 0 5 】

また、著作権を有するデータが不正にコピーされるのを防ぐ別の例としては、Digital Versatile Disk (DVD) (商標) システムにおける、コンテンツスクランブルシステムがあげられる。このシステムでは、ディスク上の、著作権を有するデータが全て暗号化され、ライセンスを受けた記録装置だけが暗号鍵を与えられ、これにより暗号化されたデータを復号し、意味のあるデータを得ることができ

るようになされている。そして、記録装置は、ライセンスを受ける際に、不正コピーを行わない等の動作規定に従うように設計される。このようにして、DVDシステムにおいては、著作権を有するデータが不正にコピーされるのを防いでいる。

【0006】

【発明が解決しようとする課題】

上記のミニディスクシステムが採用している方式では、SCMSがcopy once allowedであれば、これをcopy prohibitedに変更し、受信したデータとともに記録するなどの動作規定に従わない記録装置が、不正に製造されてしまう。

【0007】

また、上記のDVDシステムが採用している方式は、ROMメディアに対しては有効であるが、ユーザがデータを記録可能なRAMメディアにおいては有効ではない。RAMメディアにおいては、不正者は、暗号を解読できない場合であっても、ディスク上のデータを全部、新しいディスクに不正にコピーすることによって、ライセンスを受けた正当な記録装置で動作するディスクを新たに作ることができるからである。

【0008】

そこで、本件出願人が先に出願した特願平 1 0 - 2 5 3 1 0 号の特許出願においては、個々の記録媒体を識別するための情報（以下、媒体識別情報とよぶ）を記録媒体に持たせ、この情報はライセンスを受けた装置しかアクセスできないようにしている。すなわち、記録媒体上のデータは媒体識別情報と、ライセンスを受けることによって得られる秘密に基づく鍵によって暗号化し、ライセンスを受けていない装置はデータを読み出しても意味のないものとしている。さらに装置にライセンスを与える際にはその動作を規定し、不正コピーを行わないようにする。ライセンスを得ていない装置は媒体識別情報にアクセスできず、また媒体識別情報は個々の媒体ごとに個別の値になっているため、ライセンスを受けていない装置がアクセス可能なすべての情報を新たな媒体にコピーしたとしても、そのようにして作られた媒体は、ライセンスを受けていない装置でもライセンスを受けた装置でも正しく情報が読み出せないようにしている。

【0 0 0 9】

しかしながら、ある記録装置によって情報が記録された記録媒体が、他の装置で再生可能であることを保証するために、記録媒体上のデータを暗号化する暗号鍵は、システム全体で共通の秘密（マスターキー）に基づいて生成されるようになっている。これはすなわち、一つの装置が攻撃されてマスターキーが露呈してしまうと、そのシステムの任意の装置によって記録されたすべてのデータの暗号が解かれ、システム全体が壊滅する恐れがあることを意味している。

【0 0 1 0】

そこで、本発明の目的は、暗号鍵を安全に保管することができるようにした情報記録／再生システム、情報記録／再生装置、情報記録／再生方法及び情報記録媒体を提供することにある。

【0 0 1 1】

また、本発明の他の目的は、不正な機器にデータを漏らすことのないようにした情報記録／再生システム、情報記録／再生装置、情報記録／再生方法及び情報記録媒体を提供することにある。

【0 0 1 2】

また、本発明の他の目的は、正当な機器だが攻撃されてその機器の秘密が露呈してしまった機器にデータを与えることも防ぐことができるようにした情報記録／再生システム、情報記録／再生装置、情報記録／再生方法及び情報記録媒体を提供することにある。

【0 0 1 3】

さらに、本発明の他の目的は、映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことができるようにした情報記録／再生システム、情報記録／再生装置、情報記録／再生方法及び情報記録媒体を提供することにある。

【0 0 1 4】

【課題を解決するための手段】

本発明では、情報記録媒体にセキュリティモジュールを持たせる。情報記録媒体上に記録されるデータは、個々のデータごとに異なる暗号鍵で暗号化され、暗

号鍵はセキュリティモジュールが安全に保管する。また、セキュリティモジュールは記録／再生装置と公開鍵暗号技術を用いた相互認証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにする。さらに、信頼できるセンタが発行するリボケーションリストを活用することにより、正当な装置だが攻撃されてその装置の秘密が露呈してしまった装置にデータを与えることも防ぐことができるようにする。

【0015】

すなわち、本発明に係る情報記録／再生システムは、セキュリティモジュールを有する情報記録媒体と、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体に記録、あるいは、上記セキュリティモジュールが管理する暗号鍵によって暗号化されたデータを上記情報記録媒体から再生する情報記録／再生装置とを備え、情報記録時、又は情報再生時に上記情報記録／再生装置とセキュリティモジュールとが公開鍵暗号技術を用いた相互認証プロトコルを実行することを特徴とする。

【0016】

また、本発明に係る情報記録媒体は、データの記録時及び再生時に、情報記録／再生装置との間で公開鍵暗号を用いた相互認証プロトコルを実行するセキュリティモジュールを有することを特徴とする。

【0017】

また、本発明に係る情報記録／再生装置は、データの記録時及び再生時に、情報記録媒体のセキュリティモジュールとの間で公開鍵暗号を用いた相互認証プロトコルを実行する制御手段を備えることを特徴とする。

【0018】

また、本発明は、情報記録／再生装置により情報記録媒体にデータを記録、あるいは情報記録媒体からデータを再生する情報記録／再生方法において、情報記録媒体が有するセキュリティモジュールと情報記録／再生装置が公開鍵暗号を用いた相互認証プロトコルを実行するステップを有することを特徴とする。

【 0 0 1 9 】

さらに、本発明に係る情報記録媒体は、外部装置とインタフェースをとるためのインタフェース機能と、乱数を生成するための乱数生成機能と、情報を保存するための記憶機能と、公開鍵暗号技術を用いた相互認証プロトコルに必要な計算を行う演算機能を有するセキュリティモジュールを備えることを特徴とする。

【 0 0 2 0 】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。

【 0 0 2 1 】

図 1 は、本発明を適用した光ディスク情報記録媒体 1 0 の構成例を示している

【 0 0 2 2 】

この光ディスク情報記録媒体 1 0 は、カートリッジ 1 1 内に、データを記録する光ディスク 1 2 と、セキュリティモジュール 1 3 を備えている。図 2 は、上記セキュリティモジュール 1 3 の構成例を示している。

【 0 0 2 3 】

セキュリティモジュール 1 3 は、図 2 に示すように、モジュール外の装置とデータの授受をするための接触式あるいは非接触式のインタフェース部 3 1、演算を行うための演算部 3 2、疑似乱数を発生させる乱数発生部 3 3、不揮発性メモリ 3 4 と、それらを制御するための制御部 3 5 を備えている。

【 0 0 2 4 】

図 3 は、本発明を適用した光ディスク記録／再生装置 1 0 0 の構成例を示している。

【 0 0 2 5 】

この光ディスク記録／再生装置 1 0 0 は、上記光ディスク情報記録媒体 1 0 を介してデータの記録／再生を行うもので、カートリッジ 1 1 内の光ディスク 1 2 を回転させるスピンドルモータ 1 0 1、光学ヘッド 1 0 2、サーボ回路 1 0 3、記録／再生回路 1 0 4、これらを制御する制御部 1 0 5、この制御部 1 0 5 に接続された入力部 1 0 6、乱数発生部 1 0 7 やインタフェース部 1 0 8 など

ている。

【0026】

スピンドルモータ101は、サーボ回路103によって制御され、光ディスク12を回転させる。光学ヘッド102は、レーザビームを光ディスク12に照射することで、データの記録／再生を行う。サーボ回路103は、スピンドルモータ101を駆動することにより、光ディスク12を所定の速度で（例えば線速度一定で）回転させる。また、サーボ回路103は、光学ヘッド102のトラッキング及びフォーカシングの他、スレッドサーボを制御する。

【0027】

そして、記録／再生回路104は、制御部105により動作モードが切り換えられる暗号化部104Aと復号部104Bを有する。暗号化部104Aは、記録モード時に、外部から記録信号の供給を受け取ると、これを暗号化し、光学ヘッド102に供給して、光ディスク12に記録させる。復号部104Bは、再生モード時に、光学ヘッド102により光ディスク12から再生されたデータを復号し、外部に再生信号として出力する。

【0028】

また、入力部106は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより入力操作されたとき、その入力操作に対応する信号を出力する。制御部105は、記憶されている所定のコンピュータプログラムに従って、装置全体を制御する。乱数発生部107は、制御部105の制御により、所定の乱数を発生する。インタフェース108部は、接触式あるいは非接触式であり、情報記録媒体10のセキュリティモジュール13とデータの授受を行う。

【0029】

さらに、この光ディスク記録／再生装置100は、演算部109と不揮発性メモリ110を備えている。

【0030】

光ディスク情報記録媒体10のセキュリティモジュール13と光ディスク記録／再生装置100は、1台ごとに個別の識別コード(ID)と、IDに対応する公開鍵暗号系の秘密鍵と公開鍵、さらに、公開鍵証明書を信頼できるセンタ(Trust

ed Center: TC)から与えられており、それぞれの不揮発性メモリ 3 4, 1 1 0 にこれらを格納しておく。特に、秘密鍵は外部に漏れないように安全に格納する。

【0 0 3 1】

ここで、公開鍵証明書は、IDと公開鍵を含む情報にTCがデジタル署名を施したデータである。

【0 0 3 2】

また、デジタル署名技術は、あるデータを生成したのがあるユーザであることを証明できる技術であり、例えばIEEE P 1 3 6 3 で使用されているElliptic Curve Digital Signature Algorithm (EC-DSA) 方式などがよく知られている。

【0 0 3 3】

この実施の形態では、公開鍵証明書に含まれるTCのデジタル署名を検証するために、システム全体で共通であるTCの公開鍵を光ディスク情報記録媒体 1 0 と光ディスク記録／再生装置 1 0 0 の不揮発性メモリ 3 4, 1 1 0 に格納する。

【0 0 3 4】

上記光ディスク情報記録媒体 1 0 のセキュリティモジュール 1 3 と光ディスク記録／再生装置 1 0 0 は、その不揮発メモリ 3 4, 1 1 0 に、図 4 に示すリボケーションリストを格納する領域を有する。

【0 0 3 5】

リボケーションリストは、単調増加であるそのバージョンナンバーと、秘密鍵が露呈した光ディスク情報記録媒体あるいは光ディスク記録／再生装置のIDにTCがデジタル署名を施したものである。

【0 0 3 6】

光ディスク情報記録媒体 1 0 のセキュリティモジュール 1 3 の不揮発メモリ 3 4 の容量が小さく、リボケーションリストを格納できない場合には、不揮発メモリ 3 4 ではなく、光ディスク 1 2 部分にリボケーションリストを格納してもよい。

【0 0 3 7】

光ディスク記録／再生装置 1 0 0 は、それが工場から出荷される際に、最新版

のリボケーションリストを与えられ不揮発性メモリ 110 に格納することが望ましい。

【0038】

次に、図5を用いて、光ディスク記録／再生装置 100 が光ディスク情報記録媒体 10 にデータを記録する手順を説明する。

【0039】

光ディスク記録／再生装置 100 と光ディスク情報記録媒体 10 のセキュリティモジュール 13 は、それぞれ、TC から与えられた ID、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書と、リボケーションリストを持っている。

【0040】

まず、光ディスク記録／再生装置 100 が光ディスク情報記録媒体 10 のセキュリティモジュール 13 に対し、これからデータの記録を行うことを示す記録コマンドと、1回1回の記録を識別するために個別に割り当てる Recording-ID を送る（手順 R1）。

【0041】

上記記録コマンドをトリガーとして、光ディスク記録／再生装置 100 が光ディスク情報記録媒体 10 のセキュリティモジュール 13 は、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する（手順 R2）。

【0042】

公開鍵暗号技術を用いた相互認証プロトコルは、相手の装置が正しい（TC から承認を得た）公開鍵と秘密鍵のペアを持っていることをお互いに確認するプロトコルであり、例えば IEEE P1363 で規格化作業中の Elliptic Curve Digital Signature Algorithm (EC-DSA) を用いることによって構成することができる。

【0043】

上記公開鍵暗号技術を用いた相互認証プロトコルにおいては、双方の装置が、乱数発生機能を用いて乱数を発生させること、不揮発性メモリに格納されている自己の秘密鍵及び公開鍵証明書を読み出すこと、公開鍵暗号技術に基づく演算を演算機能で行うこと、が必要となる。

【 0 0 4 4 】

なお、公開鍵暗号技術を用いた相互認証プロトコルに対し、共通鍵暗号技術を用いた相互認証プロトコルも広く知られているが、これはその名の通り、プロトコルを行う 2 者が共通の鍵を持っていることを前提とするプロトコルである。共通鍵暗号技術を用いた相互認証プロトコルを採用しようとした場合、記録鍵体と記録／再生装置のインターオペラビリティを確保する必要があるため、システム全体で共通の鍵をすべてのセキュリティモジュール 1 3 と光ディスク記録／再生装置 1 0 0 が持つ必要がある。この場合、ひとつのセキュリティモジュールあるいは光ディスク記録／再生装置が攻撃を受けて鍵が露呈してしまうと、その影響がシステム全体に広まってしまうという問題がある。

【 0 0 4 5 】

これに対し、公開鍵暗号技術を用いた相互認証プロトコルにおいては、各装置及び各セキュリティモジュールが持つ鍵は個別であり、しかも後述のリボケーションリストを使用できるため、ひとつの装置の鍵が露呈したとしても、その装置だけをシステムから排除することができるので、影響が小さく押さえられるという利点がある。

【 0 0 4 6 】

公開鍵暗号技術を用いた鍵共有プロトコルは、2 者間で安全に秘密情報を共有するためのプロトコルであり、やはり I E E E P 1 3 6 3 で規格化作業中の Elliptic Curve Diffie Hellman (EC-DH) を用いることによって構成することができる。

【 0 0 4 7 】

公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実際に用いている例としては、I E E E 1 3 9 4 パス上のコンテンツプロテクション方式のひとつである、ソニー、松下、日立、東芝、インテルの 5 社によって開発された、Digital Transmission Content Protection 規格（この規格そのものはライセンスを受けないと見ることはできないが、その概要を記した White Paper を、ライセンス組織である Digital Transmission Licensing Administrator (DTLA) のウェブページである <http://www.dtcp.com> から誰でも取得することが可能である）の F

ull Authentication and Key Exchange プロトコルを挙げることができる。このプロトコルは、おおまかには、下記のステップ S 1 ~ S 4 で構成される。

【0048】

(S 1) 乱数発生器を用いて乱数を発生させ、不揮発性メモリから読み出した自分の公開鍵証明書とともに他方に送る。

(S 2) 相手の公開鍵証明書の正当性を公開鍵暗号技術に基づく演算を行って確かめる。

(S 3) 鍵共有のための、公開鍵暗号技術に基づく演算（第 1 段階）を行い、公開鍵暗号技術に基づく演算を行って作成した自分のデジタル署名文とともに相手に送る。

(S 4) 相手から送られた S 3. のデータについて、公開鍵暗号技術に基づく演算を行って相手のデジタル署名の検証を行い、鍵共有のための、公開鍵暗号技術に基づく演算（第 2 段階）を行って共有鍵の値を計算する。

【0049】

本方式においては、相互認証を行う際に、相手の装置が正しい秘密鍵、公開鍵ペアを持っていることのみならず、自分が持つリボケーションリスト（ブラックリスト）に相手の装置の ID があげられていないことを確認する。これにより、出荷時には正当に鍵を持っていたが、それが例えばリバースエンジニアリングなどの攻撃を受け、鍵が露呈してしまった装置の ID がリボケーションリストに載せられているので、データを渡してはいけない装置にはデータを渡さずにすむようになる。

【0050】

さらに、自分が持っているリボケーションリストのバージョンナンバーを交換する。

【0051】

もし何れかの装置が他方のリボケーションリストより新しいリボケーションリストを持っていた場合、その装置は自分のリボケーションリストを他方に送る。古いリボケーションリストを持っている装置は新しいものを持っている装置からリボケーションリストを送ってもらい、その正当性を検証した後で自分が持つリ

ボケーションリストを送られた新しいものに更新する。

【0052】

なお、このリボケーションリストの送付は、後述のデータの記録と順序が前後してもかまわない。

【0053】

さて、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルの結果、光ディスク記録／再生装置100とセキュリティモジュール13は、安全にある値を共有する。

【0054】

この共有される値をSession key (Kse) と呼ぶことにする。

【0055】

次に、データを暗号化する暗号鍵 (Content key, Kc) を決定するが、この方法には、例えば、次の方法(1)～(4)のうちのひとつを用いればよい。

【0056】

(1) $Kse = Kc$ とする。セキュリティモジュール13はKcを安全にその内部の不揮発性メモリ34に格納するか、セキュリティモジュール13があらかじめ格納している鍵 (Storage key, Kst) を用いてKcを暗号化した値Enc (Kst, Kc) を光ディスク記録／再生装置100に送り、光ディスク12に記録させる。

(2) セキュリティモジュール13があらかじめ格納している鍵 (Storage key, Kst) をKcとする。この場合、セキュリティモジュール13がKstをKseで暗号化して光ディスク記録／再生装置100に送る。

(3) セキュリティモジュール13がそのデータ用のKcを乱数発生器などを用いて新たに発生させる。この場合、セキュリティモジュール13がKcをKseで暗号化して光ディスク記録／再生装置100に送る。セキュリティモジュール13はKcを安全にその内部の不揮発性メモリ34に格納するか、セキュリティモジュール13があらかじめ格納している鍵 (Storage key, Kst) を用いてKcを暗号化した値Enc (Kst, Kc) を光ディスク記録／再生装置100に送り、光ディスク12に記録させる。

(4) 光ディスク記録／再生装置 100 がそのデータ用の K_c を乱数発生器などを用いて新たに発生させる。この場合、光ディスク記録／再生装置 100 が K_c を K_{se} で暗号化してセキュリティモジュール 13 に送る。セキュリティモジュール 13 は K_c を安全にその内部の不揮発性メモリ 34 に格納するか、セキュリティモジュール 13 があらかじめ格納している鍵 (Storage key, K_{st}) を用いて K_c を暗号化した値 $Enc(K_{st}, K_c)$ を光ディスク記録／再生装置 100 に送り、光ディスク 13 に記録させる。

【0057】

上記方法 (1) ~ (4) のいずれかを用いて K_c を決定したら、光ディスク記録／再生装置 100 は記録媒体に記録するデータを K_c で暗号化し、暗号化されたデータ $Enc(K_c, data)$ を光ディスク 12 に記録する (手順 R3)。

【0058】

また、上記 K_c 又は暗号化した K_c をセキュリティモジュール 13 の不揮発性メモリ 34 又は光ディスク 12 に記録する際には、Recording-ID を検索用のキーとするために一緒に記録したり、データが記録される光ディスク 12 のセクタと同一のセクタに暗号化した K_c を記録するなどして、データと K_c の対応がとれるようにしておく。なお、この K_c の管理、伝送とデータの暗号化には、その処理速度の観点から共通鍵暗号アルゴリズムを使用することが考えられる。

【0059】

共通鍵暗号アルゴリズムは、暗号化と復号の処理に同一の暗号鍵を用いる暗号アルゴリズムであり、FIPS 46-2 で米国の標準に指定されている Data Encryption Standard (DES) をその例として挙げることできる。

【0060】

また、上記方法 (4) の場合には、光ディスク記録／再生装置 100 が K_c を決められるため、光ディスク記録／再生装置 100 はあらかじめデータを暗号化しておくことが可能になる。

【0061】

以上の手順を用いて、データを光ディスク 12 に記録する。

【 0 0 6 2 】

次に、図 6 を用いて、光ディスク記録／再生装置 1 0 0 が光ディスク 1 2 からデータを再生する手順を説明する。

【 0 0 6 3 】

光ディスク記録／再生装置 1 0 0 と光ディスク記録媒体 1 0 のセキュリティモジュール 1 3 は、それぞれ TC から与えられた ID、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書と、リボケーションリストを持っている。

【 0 0 6 4 】

また、光ディスク記録／再生装置 1 0 0 は、再生すべきデータに付与された Recording-ID を知っているものとする。

【 0 0 6 5 】

まず、光ディスク記録／再生装置 1 0 0 がセキュリティモジュール 1 3 に対し、これからデータの再生を行うことを示す再生コマンドと Recording-ID を送る（手順 P 1）。

【 0 0 6 6 】

上記再生コマンドをトリガーとして、光ディスク記録／再生装置 1 0 0 とセキュリティモジュール 1 3 は公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを行う（手順 P 2）。

【 0 0 6 7 】

このプロトコルの内容は、データの記録時に行うものと同様であり、他方の装置が持つ公開鍵、秘密鍵が正しいことの検証、リボケーションリストに ID が載せられていないことの確認をお互に行い、Session key (K_{se}) を共有し、また自分が持つリボケーションリストのバージョンナンバーを送り合う。どちらかの装置が相対的に新しいリボケーションリストを持っていた場合には、それを他方の装置に送り、送られた装置はそれを用いて自分のリボケーションリストを更新することも同様である。また、リボケーションリストを送る処理が下記のデータの読み出しと前後してよいことも同様である。

【 0 0 6 8 】

次に、データを光ディスク 1 2 から読み出す前に、このデータを暗号化してい

る暗号鍵 K_c を光ディスク記録／再生装置 100 が知ることが必要になる。

【0069】

K_c は、セキュリティモジュール 13 が安全にその内部の不揮発性メモリ 34 に格納しているか、セキュリティモジュール 13 があらかじめ格納している鍵 (Storage key、 K_{st}) を用いて K_c を暗号化した値 $E_{nc}(K_{st}, K_c)$ が光ディスク 12 に記録されている。

【0070】

前者の場合であれば、セキュリティモジュール 13 は不揮発性メモリ 34 に格納されている K_c を K_{se} で暗号化して光ディスク記録／再生装置 100 に送り、光ディスク記録／再生装置 100 が K_{se} でこれを復号して K_c を得る。

【0071】

後者の場合であれば、光ディスク記録／再生装置 100 は、光ディスク 12 から $E_{nc}(K_{st}, K_c)$ を読み出し、これをセキュリティモジュール 13 に送る。セキュリティモジュール 13 は K_{st} を用いてこれを復号して K_c を得、これを K_{se} で暗号化した $E_{nc}(K_{se}, K_c)$ を光ディスク記録／再生装置 100 に送る。光ディスク記録／再生装置 100 はこれを K_{se} で復号して K_c を得る。

【0072】

このようにして、光ディスク記録／再生装置 100 は、データを暗号化している暗号鍵 K_c を得ることができる。

【0073】

次に、光ディスク記録／再生装置 100 は光ディスク 12 から K_c を用いて暗号化されているデータ $E_{nc}(K_c, \text{data})$ を読み出し、 K_c を用いてこれを復号し使用する (手順 P3)。

【0074】

以上が、光ディスク 12 からデータを読み出す処理である。

【0075】

次に、本発明の別の実施の形態を説明する。

【0076】

図 7 は、本発明を適用した不揮発性メモリ情報記録媒体 20 の構成例を示して

いる。

【 0 0 7 7 】

この不揮発性メモリ情報記録媒体 2 0 は、カートリッジ 2 1 内に、データを記録する電氣的に消去可能な不揮発性メモリ（具体的には例えば、Flash ROM や EE PROM など） 2 2 と、セキュリティモジュール 2 3 を備えている。

【 0 0 7 8 】

上記セキュリティモジュール 2 3 は、その構成例を図 8 に示すように、外部インタフェース部 4 1、演算部 4 2、乱数発生部 4 3、不揮発性メモリ 4 4、制御部 4 5、記録媒体インタフェース部 4 6 からなる。

【 0 0 7 9 】

すなわち、このセキュリティモジュール 2 3 は、図 2 に示したセキュリティモジュール 1 3 とほぼ同じ構成であるが、図 2 のインタフェース部 3 1 はこのセキュリティモジュール 2 3 では外部インタフェース部 4 1 とし、外部装置とのインタフェースとなっている。

【 0 0 8 0 】

また、カートリッジ 2 1 内の不揮発性メモリ 2 2 とのインタフェースをとるための記録媒体インタフェース（例えば、Flash ROM インタフェース） 4 6 を持ち、不揮発性メモリ 2 2 への情報の記録（書き込み）、再生（読み出し）はセキュリティモジュール 2 3 を介して行われる。

【 0 0 8 1 】

セキュリティモジュール 2 3 内部の不揮発性メモリ 4 4 は、秘密性の必要な情報や耐改ざん性が必要な情報など、重要な情報を格納するのに用いられるが、もしこのメモリ 4 4 の容量が十分でない場合には、セキュリティモジュール 2 3 外の、一般データを記録するための不揮発性メモリ 2 2 にこれらの重要な情報を記録することもできる。この場合、秘密性の必要な情報については、セキュリティモジュール 2 3 内の不揮発性メモリ 4 4 に安全に格納してある storage key を鍵として暗号化するなどの方法を用いて保護し、耐改ざん性の必要な情報については、重要な情報を記録する不揮発性メモリ 2 2 のブロックの Integrity Check Value (ICV) を計算し、セキュリティモジュール 2 3 内の不揮発性メモリ 4 4 に格

納しておき、セキュリティモジュール23外の不揮発性メモリ22から情報を読み出す際に再びそのブロックのICVを計算して格納してある値と比較することによって情報が改ざんされていないことを確認するなどの保護をかける。

【0082】

ICVは、あるデータのIntegrity（改ざんされていないこと）を保証するために、データと、何らかの秘密（この場合、例えばセキュリティモジュール23のstoragekey）を入力としてあらかじめ定められたアルゴリズムによって計算される値であり、上記の秘密を知っているものしか任意のデータに対するICVを計算することが事実上できないため、データが変更された場合には読み出し時に同様の方法で計算されるICVと記録時に計算されてセキュリティモジュール23内に格納されている値が異なるためデータが変更された事実をセキュリティモジュール23が知ることができる。

【0083】

ICVを計算するアルゴリズムとしては、公開鍵暗号技術を用いたデジタル署名アルゴリズムや、共通鍵暗号技術を用いたMessage Authentication Code 作成アルゴリズム、鍵つきハッシュ関数を用いるアルゴリズムなどがある。

【0084】

ICVについては、例えば、Menezesの他、「Handbook of applied cryptography」、CRC、ISBN 0-8493-8523-7、pp. 352 - 368に詳しい解説がある。

【0085】

図9は、本発明を適用した不揮発メモリ記録媒体20の記録／再生装置200の構成例を表している。この図9に示した記録／再生装置200は、入出力端子201、制御部205、入力部206、乱数発生部207、インタフェース部208、演算部209、不揮発性メモリ210などからなる。

この記録／再生装置200は、図3に示した光ディスク記録／再生装置100とほぼ同じであるが、スピンドルモータ101、光学ヘッド102やサーボ回路103など光ディスク12用の構成要素のかわりにセキュリティモジュール23にアクセスするためのインタフェース部208が、セキュリティモジュール23を介して不揮発メモリ記録媒体20への記録／再生のためのインタフェースも兼

用する。不揮発メモリ記録媒体 2 0 は、入出力端子 2 4, 2 0 1 を介して記録／再生装置 2 0 0 と電氣的に接続される。

【 0 0 8 6 】

次に、図 1 0 を用いて、記録／再生装置 2 0 0 が不揮発メモリ記録媒体 2 0 にデータを記録する手順を説明する。

【 0 0 8 7 】

図 5 で示した例と同様に、記録／再生装置 2 0 0 と不揮発メモリ記録媒体 2 0 のセキュリティモジュール 2 3 は、それぞれ、TC から与えられた ID、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書と、リボケーションリストを持っている。

【 0 0 8 8 】

まず、記録／再生装置 2 0 0 がセキュリティモジュール 2 3 に対し、これからデータの記録を行うことを示す記録コマンドと、1 回 1 回の記録を識別するために個別に割り当てる Recording-ID を送る（手順 R 1 1）。

【 0 0 8 9 】

上記記録コマンドをトリガーとして、記録／再生装置 2 0 0 とセキュリティモジュール 2 3 は公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する（手順 R 1 2）。このプロトコルの内容は、上述の光ディスク記録／再生装置 1 0 0 おけるデータの記録時に行うものと同様であり、他方の装置が持つ公開鍵、秘密鍵が正しいことの検証、リボケーションリストに ID が載せられていないことの確認を互いに行い、Session key (Kse) を共有し、また自分が持つリボケーションリストのバージョンナンバーを送り合う。どちらかの装置が相対的に新しいリボケーションリストを持っていた場合には、それを他方の装置に送り、送られた装置はそれを用いて自分のリボケーションリストを更新することも同様である。また、リボケーションリストを送る処理が下記のデータの読み出しと前後してよいことも同様である。

【 0 0 9 0 】

次に、データを暗号化する暗号鍵 (Content key, Kc) を決定するが、この方法には例えば、次の方法 (1 1) ～ (1 4) のうちのひとつを用いればよい。

【0091】

(11) $K_{se} = K_c$ とする。セキュリティモジュール23は K_c を安全にその内部の不揮発性メモリ44に格納するか、セキュリティモジュール23があらかじめ格納している鍵 (Storage key, K_{st}) を用いて K_c を暗号化した値 $E_{nc}(K_{st}, K_c)$ をモジュール23外の不揮発性メモリ22に格納する。

(12) セキュリティモジュール23があらかじめ格納している鍵 (Storage key, K_{st}) を K_c とする。この場合、セキュリティモジュール23が K_{st} を K_{se} で暗号化して記録/再生装置200に送る。

(13) セキュリティモジュール23がそのデータ用の K_c を乱数発生器などを用いて新たに発生させる。この場合、セキュリティモジュール23が K_c を K_{se} で暗号化して記録/再生装置200に送る。セキュリティモジュール23は K_c を安全にその内部の不揮発性メモリ44に格納するか、セキュリティモジュール23があらかじめ格納している鍵 (Storage key, K_{st}) を用いて K_c を暗号化した値 $E_{nc}(K_{st}, K_c)$ をモジュール23外の不揮発性メモリ22に格納する。

(14) 記録/再生装置200がそのデータ用の K_c を乱数発生器などを用いて新たに発生させる。この場合、記録/再生装置200が K_c を K_{se} で暗号化してセキュリティモジュール23に送る。セキュリティモジュール23は K_c を安全にその内部の不揮発性メモリ44に格納するか、セキュリティモジュール23があらかじめ格納している鍵 (Storage key, K_{st}) を用いて K_c を暗号化した値 $E_{nc}(K_{st}, K_c)$ をモジュール23外の不揮発性メモリ22に格納する。

【0092】

上記方法(11)～(14)のいずれかを用いて K_c を決定したら、記録/再生装置200は不揮発メモリ記録媒体20に記録するデータを K_c で暗号化し、暗号化されたデータ $E_{nc}(K_c, \text{data})$ をセキュリティモジュール23に伝送する(手順R13)。

【0093】

セキュリティモジュール23は送られた $E_{nc}(K_c, \text{data})$ をデータ用の不揮発性メモリ22に格納する。

【0094】

また上記において、Kc又は暗号化したKcをセキュリティモジュール23の不揮発性メモリ44又はデータ用の不揮発性メモリ22に記録する際には、Recording-IDを検索用のキーとするために一緒に記録したり、データが記録される不揮発性メモリのセクタと同一のセクタに暗号化したKcを記録するなどして、データとKcの対応がとれるようにしておく。

【0095】

また、上記方法(14)の場合には、記録／再生装置200がKcを決められるため、記録／再生装置200はあらかじめデータを暗号化しておくことが可能になる。

【0096】

以上の手順を用いて、データを不揮発メモリ記録媒体20に記録する。

【0097】

ところで、データの記録処理を図11のようにすることもできる。

【0098】

すなわち、記録／再生装置200は認証と鍵共有プロトコルでセキュリティモジュール23と共有したSession key (Kse) を用いてデータを暗号化してセキュリティモジュール23に送る(手順R23)。

【0099】

セキュリティモジュール23は同じくKseを用いてこれを復号し平文のデータを得、次に新たに発生させたKcで暗号化してEnc(Kc, data)をデータ用の不揮発性メモリに記録する(手順R24)。

【0100】

セキュリティモジュール23はKcを安全にその内部の不揮発性メモリ44に格納するか、セキュリティモジュール23があらかじめ格納している鍵(Storage key, Kst)を用いてKcを暗号化した値Enc(Kst, Kc)をモジュール23外の不揮発性メモリ22に格納する。このようにすると、セキュリティモジュール23はデータの暗号鍵Kcを記録／再生装置200にも教えないですむようになる。

【0101】

以上のようにして、データを記録媒体に記録することができる。

【0102】

次に、図12を用いて、記録／再生装置200が不揮発メモリ記録媒体20からデータを再生する手順を説明する。

【0103】

記録／再生装置200と不揮発メモリ記録媒体20のセキュリティモジュール23は、それぞれ、TCから与えられたID、公開鍵暗号系の秘密鍵、公開鍵、公開鍵証明書と、リボケーションリストを持っている。また、記録／再生装置200は、再生すべきデータに付与されたRecording-IDを知っているものとする。

【0104】

まず、記録／再生装置200がセキュリティモジュール23に対し、これからデータの再生を行うことを示す再生コマンドと、Recording-IDを送る（手順P11）。

【0105】

上記再生コマンドをトリガーとして、記録／再生装置200とセキュリティモジュール23は公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを実行する（手順P12）。

【0106】

このプロトコルの内容は、データの記録時に行うものと同様であり、他方の装置が持つ公開鍵、秘密鍵が正しいことの検証、リボケーションリストにIDが載せられていないことの確認をお互に行い、Session key (Kse) を共有し、また自分が持つリボケーションリストのバージョンナンバーを送り合う。どちらかの装置が相対的に新しいリボケーションリストを持っていた場合には、それを他方の装置に送り、送られた装置はそれを用いて自分のリボケーションリストを更新することも同様である。また、リボケーションリストを送る処理が下記のデータの読み出しと前後してよいことも同様である。

【0107】

次に、データを不揮発性メモリ22から読み出す前に、このデータを暗号化し

ている暗号鍵Kcを記録／再生装置に知らせる。

【0108】

Kcは、セキュリティモジュール23が安全にその内部の不揮発性メモリ44に格納しているかセキュリティモジュール23があらかじめ格納している鍵(Storage key, Kst)を用いてKcを暗号化した値Enc(Kst, Kc)がデータ用の不揮発性メモリ22に記録されている。

【0109】

前者の場合であれば、セキュリティモジュール23は不揮発性メモリ44に格納されているKcをKseで暗号化して記録／再生装置200に送り、記録／再生装置200がKseでこれを復号してKcを得る。

【0110】

後者の場合であれば、セキュリティモジュール23はデータ用の不揮発性メモリ22からEnc(Kst, Kc)を読み出し、Kstを用いてこれを復号してKcを得、これをKseで暗号化したEnc(Kse, Kc)を記録／再生装置200に送る。記録／再生装置200はこれをKseで復号してKcを得る。

【0111】

このようにして、記録／再生装置200はデータを暗号化している暗号鍵Kcを得ることができる。

【0112】

次に、記録／再生装置200はデータ用の不揮発性メモリ22からKcを用いて暗号化されているデータEnc(Kc, data)をセキュリティモジュール23を介して読み出し(手順P13)、Kcを用いてこれを復号し使用する(手順P14)。

【0113】

以上が、記録媒体からデータを読み出す処理である。

【0114】

ところで、データの再生処理を図13のようにすることもできる。

【0115】

すなわち、セキュリティモジュール23が記録／再生装置200にKcを渡すこ

とはせず、セキュリティモジュール 2 3 がデータ用の不揮発性メモリ 2 2 から暗号化されたデータ $E n c (K c, data)$ を読み出した後（手順 2 3）、 $K c$ を用いて復号して平文のデータを得、次に認証と鍵共有プロトコルで共有した Session key ($K s e$) でデータを暗号化して $E n c (K s e, data)$ を記録／再生装置 2 0 0 に送る（手順 P 2 4）。

【0 1 1 6】

記録／再生装置 2 0 0 はこれを $K s e$ を用いて復号して平文データを得、使用する（手順 P 2 5）。

【0 1 1 7】

このようにすることにより、セキュリティモジュール 2 3 はデータを暗号化している暗号鍵 $K c$ を記録／再生装置 2 0 0 に教える必要がなくなる。

【0 1 1 8】

以上のようにして、記録媒体からのデータの読み出しが行える。

【0 1 1 9】

なお、本発明を適用した情報記録媒体としては、光ディスク記録媒体 1 0 と不揮発性メモリ記録媒体 2 0 0 の例を提示したが、記録媒体はこれに限るものではなく、磁気ディスクや磁気テープ、光磁気ディスク、バッテリーバックアップされた揮発性メモリなどでもよい。

【0 1 2 0】

【発明の効果】

以上に説明したように、本発明によれば、記録媒体にセキュリティモジュールを持たせ記録媒体上に記録されるデータは個々のデータごとに異なる暗号鍵で暗号化され、暗号鍵はセキュリティモジュールが安全に保管することができる。

【0 1 2 1】

また、セキュリティモジュールは、データの記録時及び再生時に、記録／再生装置と公開鍵暗号技術を用いた相互認証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにすることができる。

【0 1 2 2】

さらに、信頼できるセンタが発行するリボケーションリストを活用することにより、正当な装置だが攻撃されてその装置の秘密が露呈してしまった装置にデータを与えることも防ぐことが可能となる。

【0 1 2 3】

このため、映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことが可能である。

【図面の簡単な説明】

【図 1】

本発明を適用した光ディスク情報記録媒体の構成を示す図である。

【図 2】

上記光ディスク情報記録媒体に備えられるセキュリティモジュールの一例を示すブロック図である。

【図 3】

本発明を適用した光ディスク情報記録／再生装置の構成を示すブロック図である。

【図 4】

リボケーションリストを説明するための図である。

【図 5】

上記光ディスク情報記録媒体にデータを記録する際の具体的な処理内容を示す図である。

【図 6】

上記光ディスク情報記録媒体からデータを再生する際の具体的な処理内容を示す図である。

【図 7】

本発明を適用した不揮発性メモリ情報記録媒体の構成を示す図である。

【図 8】

上記不揮発性メモリ情報記録媒体に備えられるセキュリティモジュールの一例を示すブロック図である。

【図 9】

本発明を適用した不揮発性メモリ情報記録／再生装置の構成を示すブロック図である。

【図 1 0】

上記不揮発性メモリ情報記録媒体にデータを記録する際の具体的な処理内容の一例を示す図である。

【図 1 1】

上記不揮発性メモリ情報記録媒体にデータを記録する際の具体的な処理内容の別の一例を示す図である。

【図 1 2】

上記不揮発性メモリ情報記録媒体からデータを再生する際の具体的な処理内容の一例を示す図である。

【図 1 3】

上記不揮発性メモリ情報記録媒体にデータを再生する際の具体的な処理内容の別の一例を示す図である。

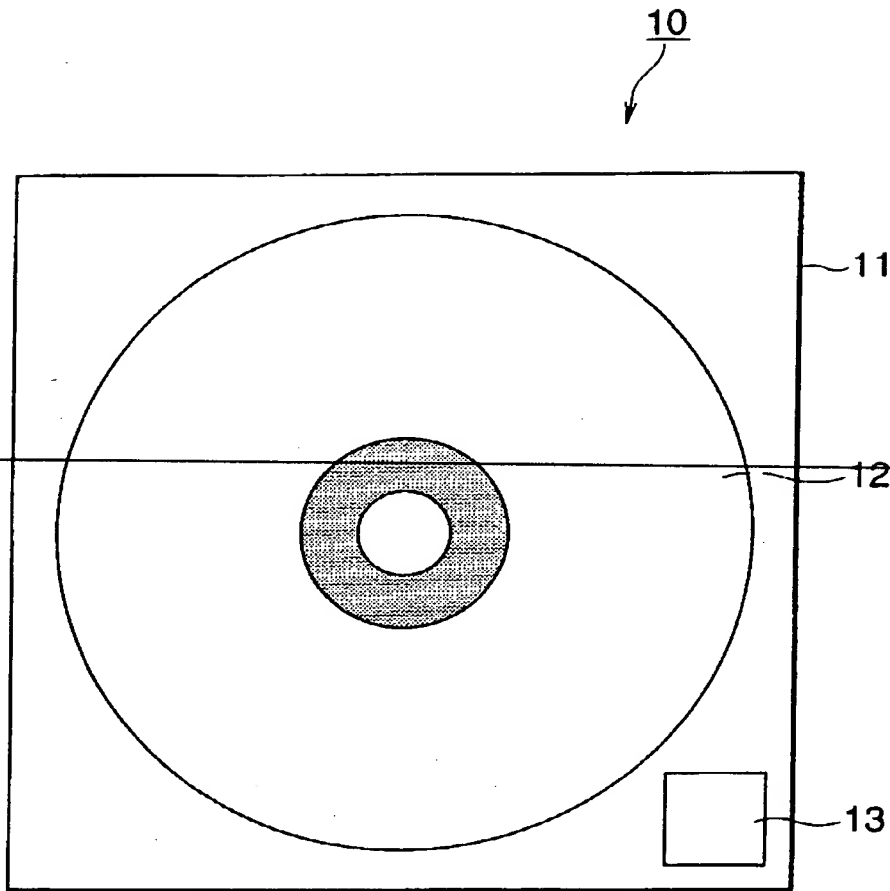
【符号の説明】

1 0 光ディスク情報記録媒体、1 1 カートリッジ、1 2 光ディスク、1 3 セキュリティモジュール、3 1 インタフェース部、3 2 演算部、3 3 乱数発生部、3 4 不揮発性メモリ、3 5 制御部、1 0 0 光ディスク記録／再生装置、1 0 1 スピンドルモータ、1 0 2 光学ヘッド、1 0 3 サーボ回路、1 0 4 記録／再生回路、1 0 5 制御部、1 0 6 入力部、1 0 7 乱数発生部、1 0 8 インタフェース部、1 0 9 演算部、1 1 0 不揮発性メモリ、2 0 不揮発性メモリ情報記録媒体、2 1 カートリッジ、2 2 不揮発性メモリ、2 3 セキュリティモジュール、2 4 入出力端子、4 1 外部インタフェース部、4 2 演算部、4 3 乱数発生部、4 4 不揮発性メモリ、4 5 制御部、4 6 記録媒体インターフェース部、2 0 0 記録／再生装置、2 0 1 入出力端子、2 0 5 制御部、2 0 6 入力部、2 0 7 乱数発生部、2 0 8 インタフェース部、2 0 9 演算部、2 1 0 不揮発性メモリ

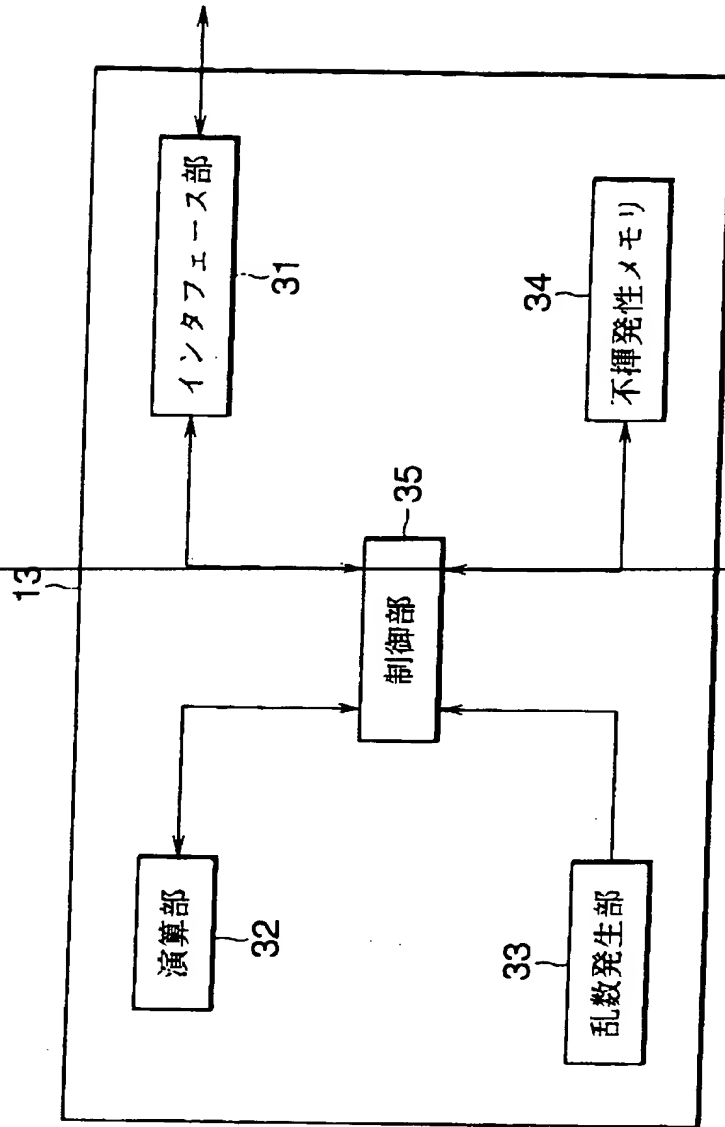
【書類名】

図面

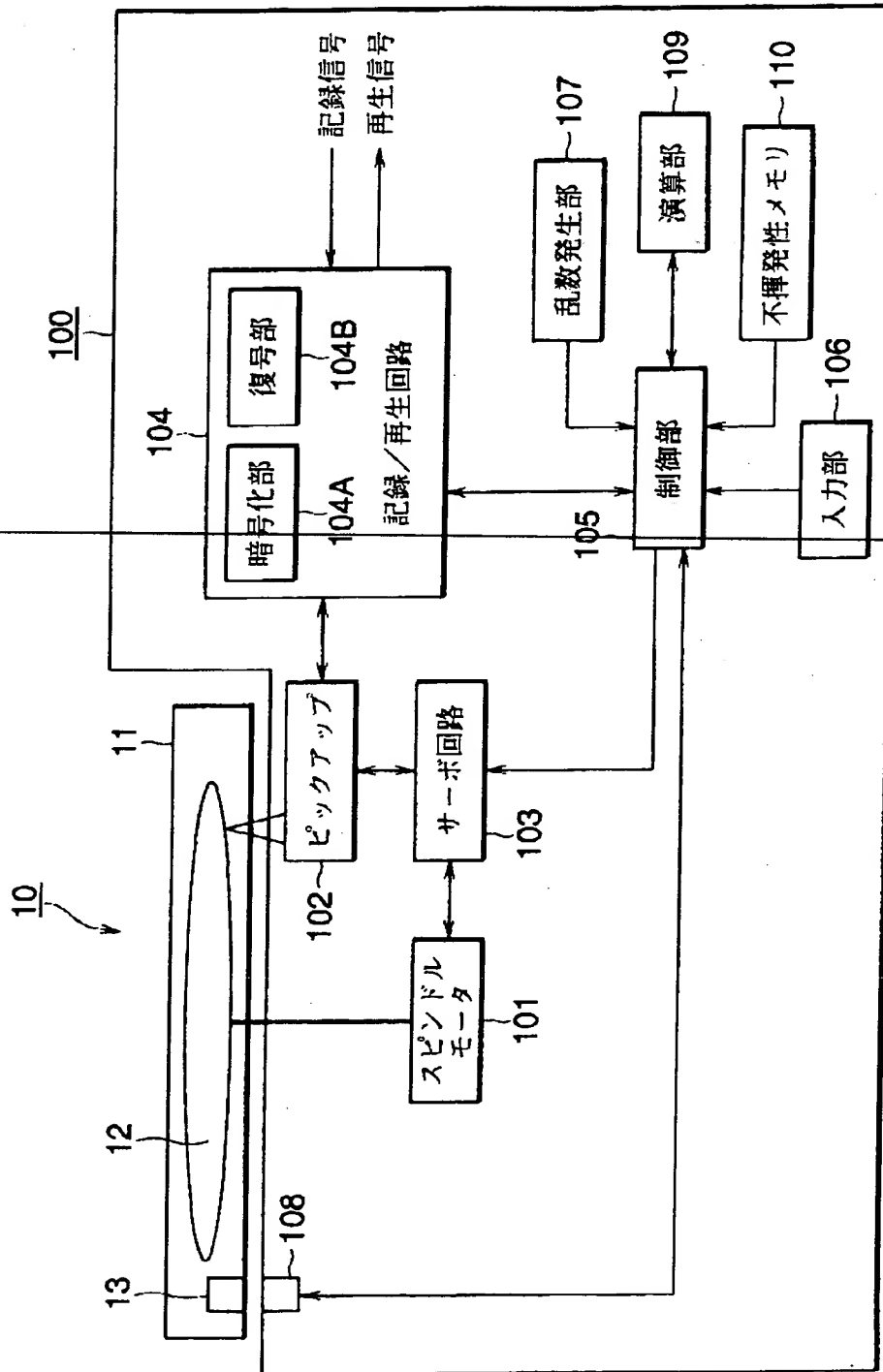
【図 1】



【図 2】



【図 3】

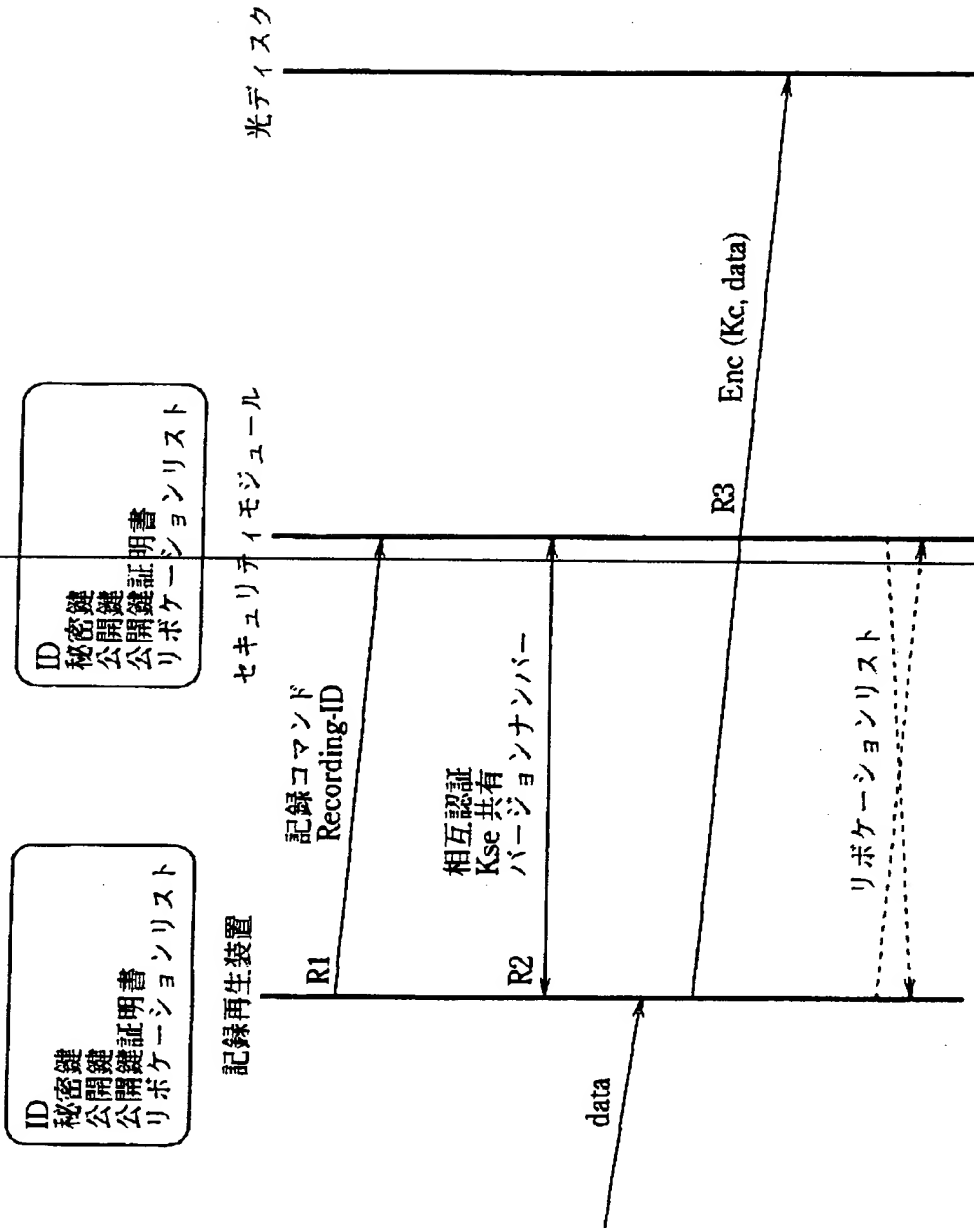


【図 4】

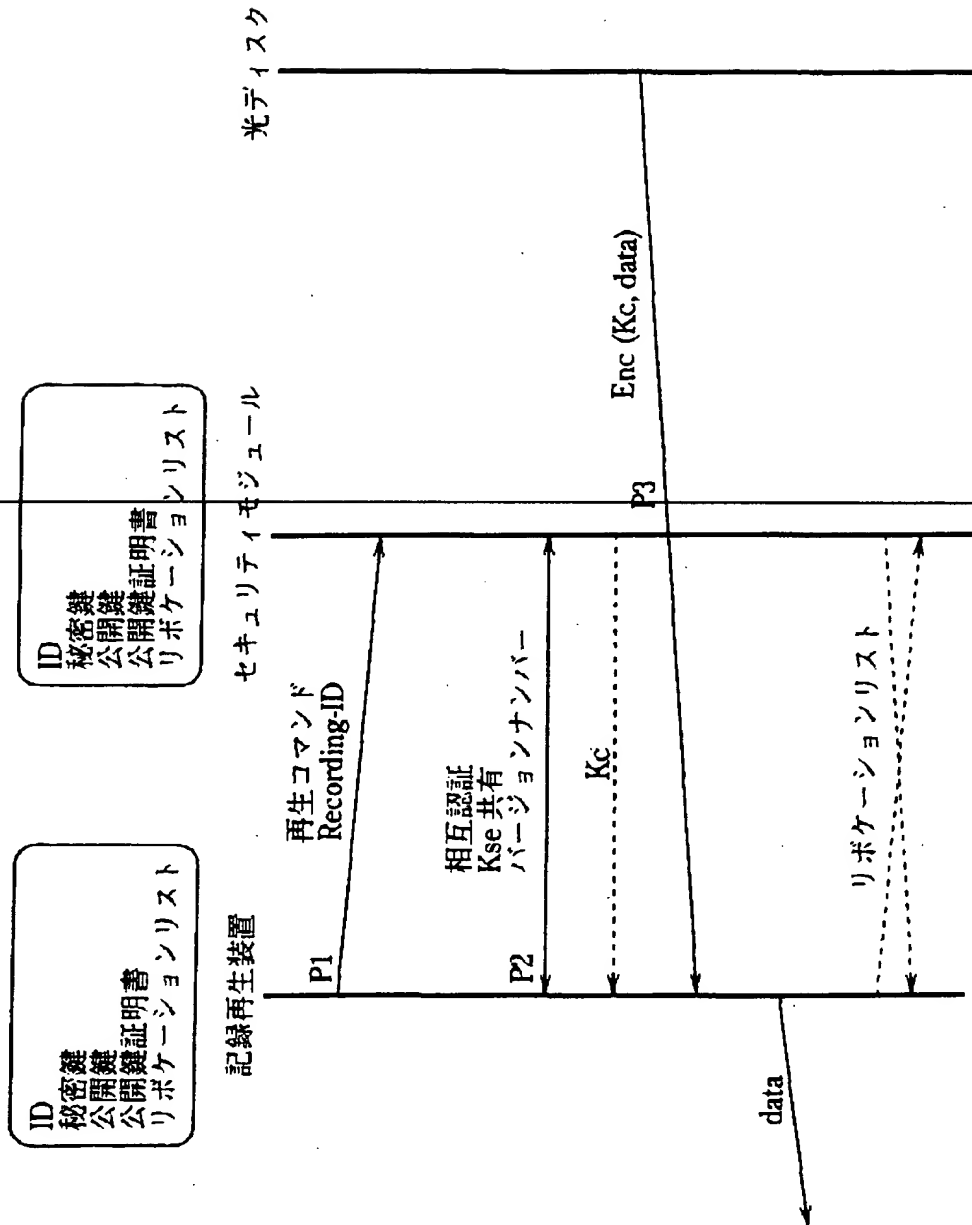
リポケーションリスト

バージョンナンバー
リポークされる機器または媒体のID
...
TC のデジタル署名

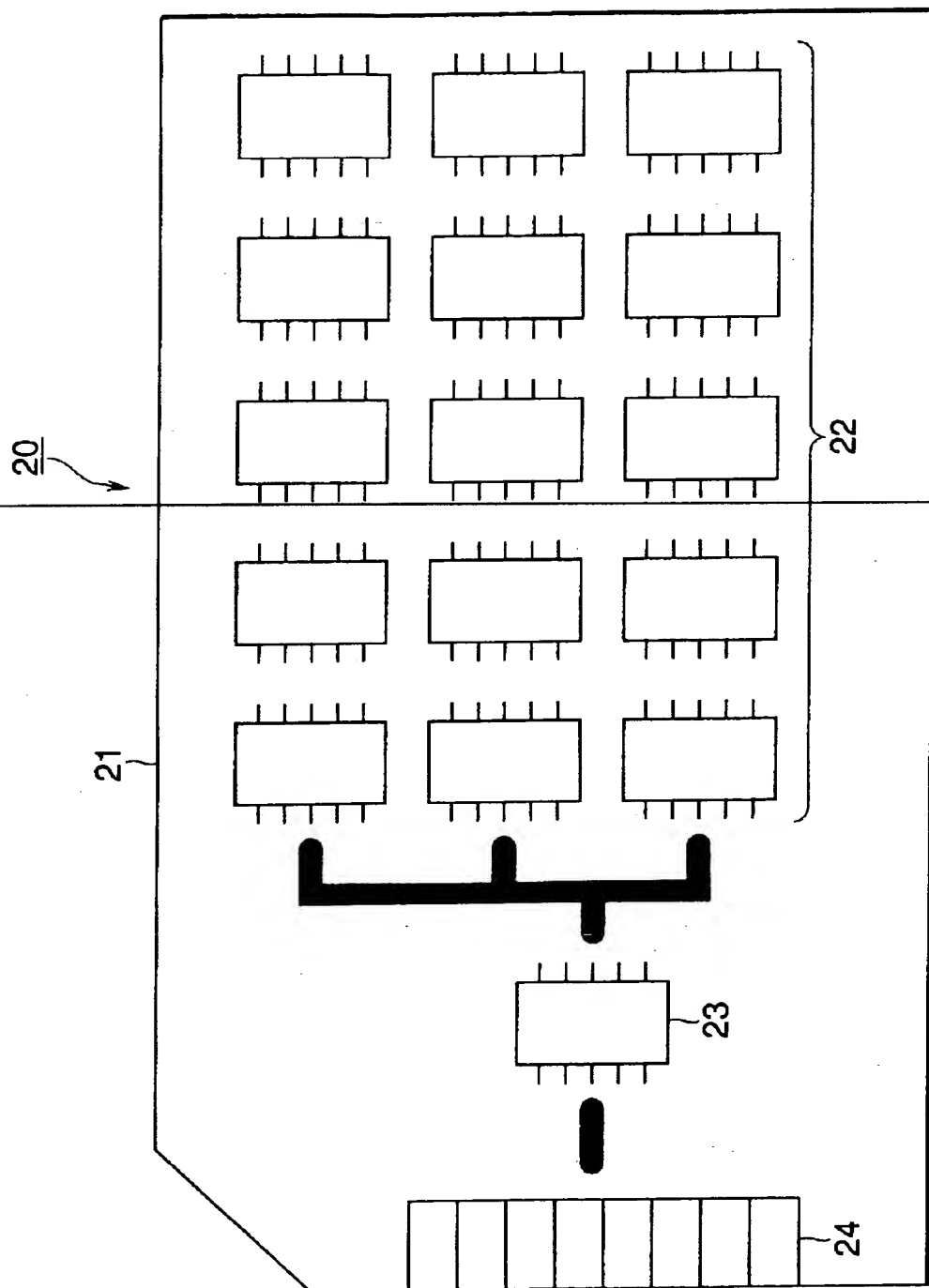
【図 5】



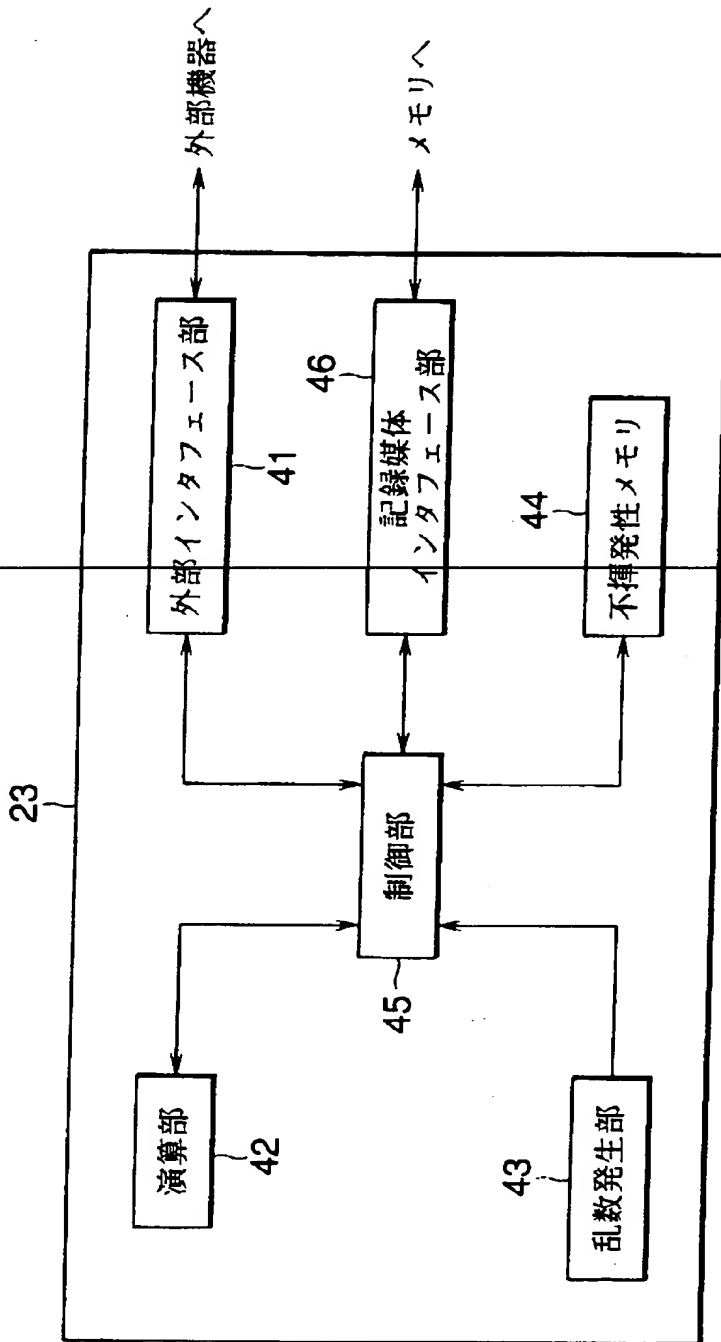
【図 6】



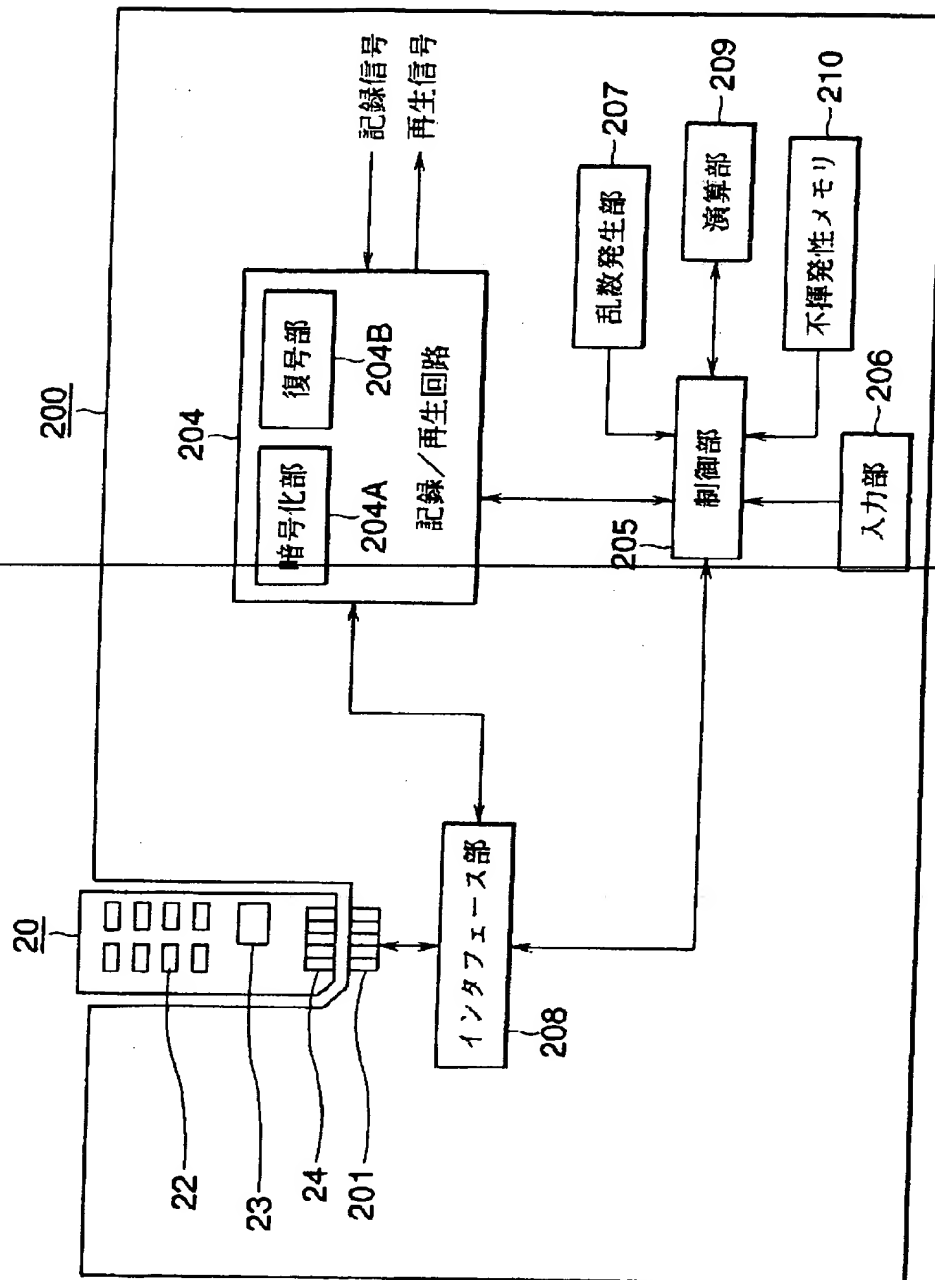
【図 7】



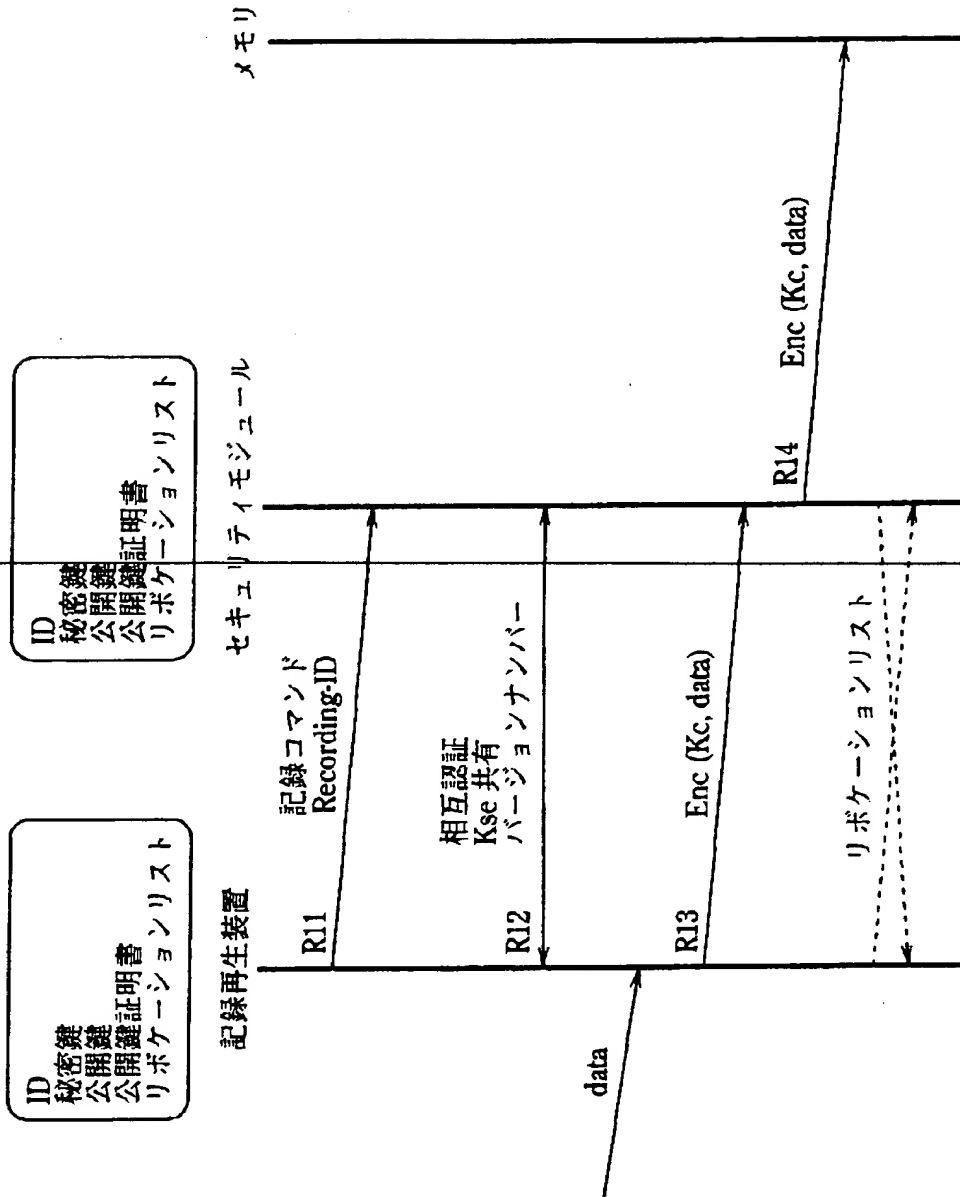
【図 8】



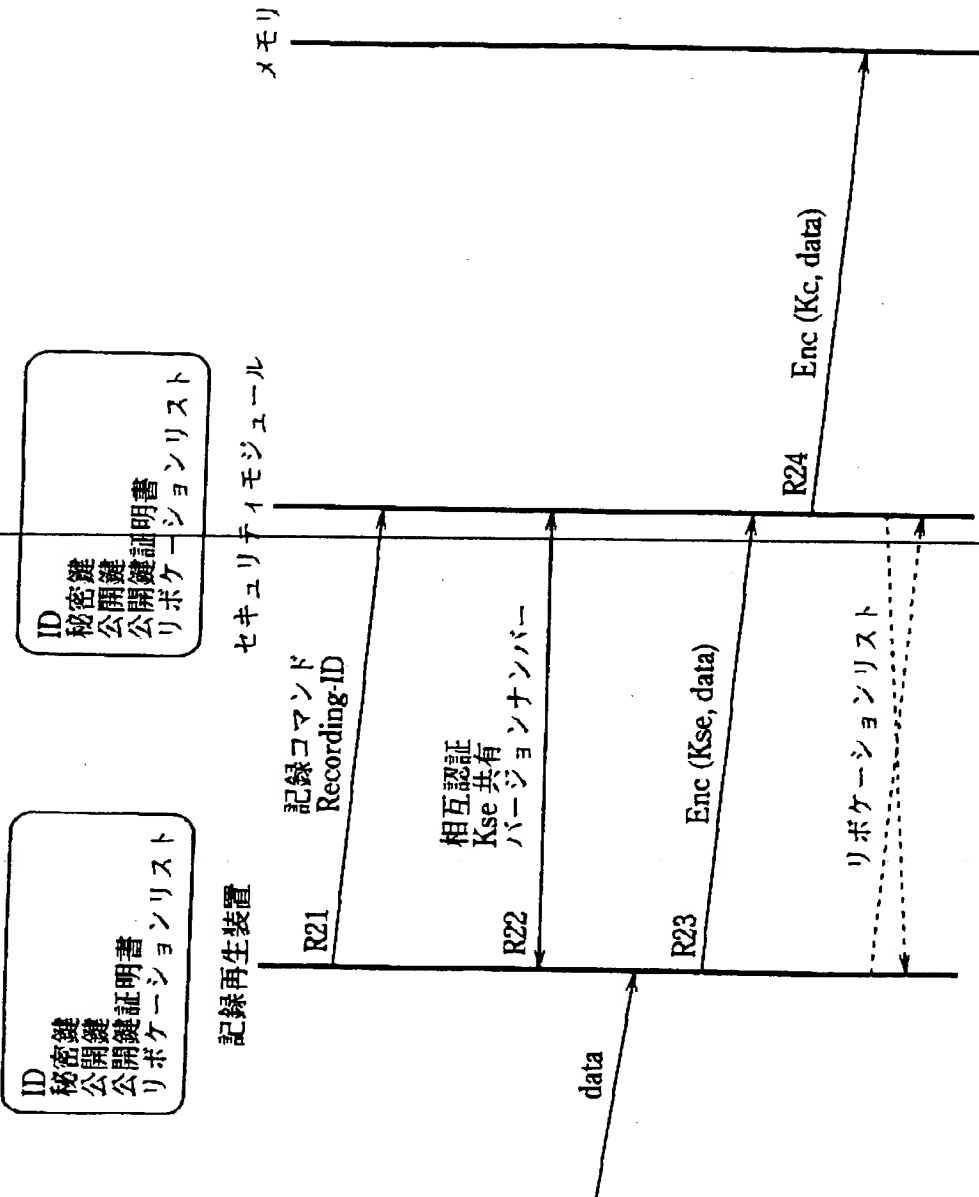
【图9】



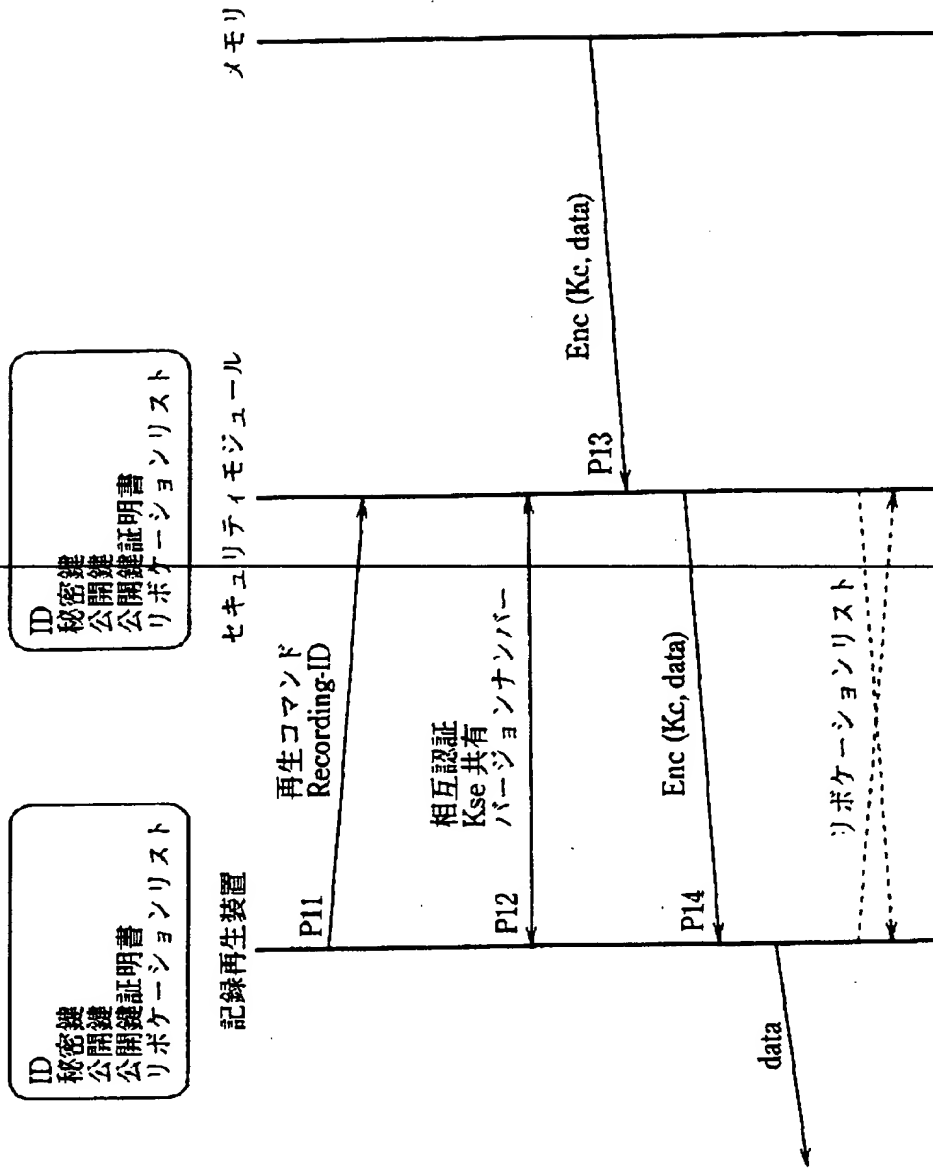
【図 1 0】



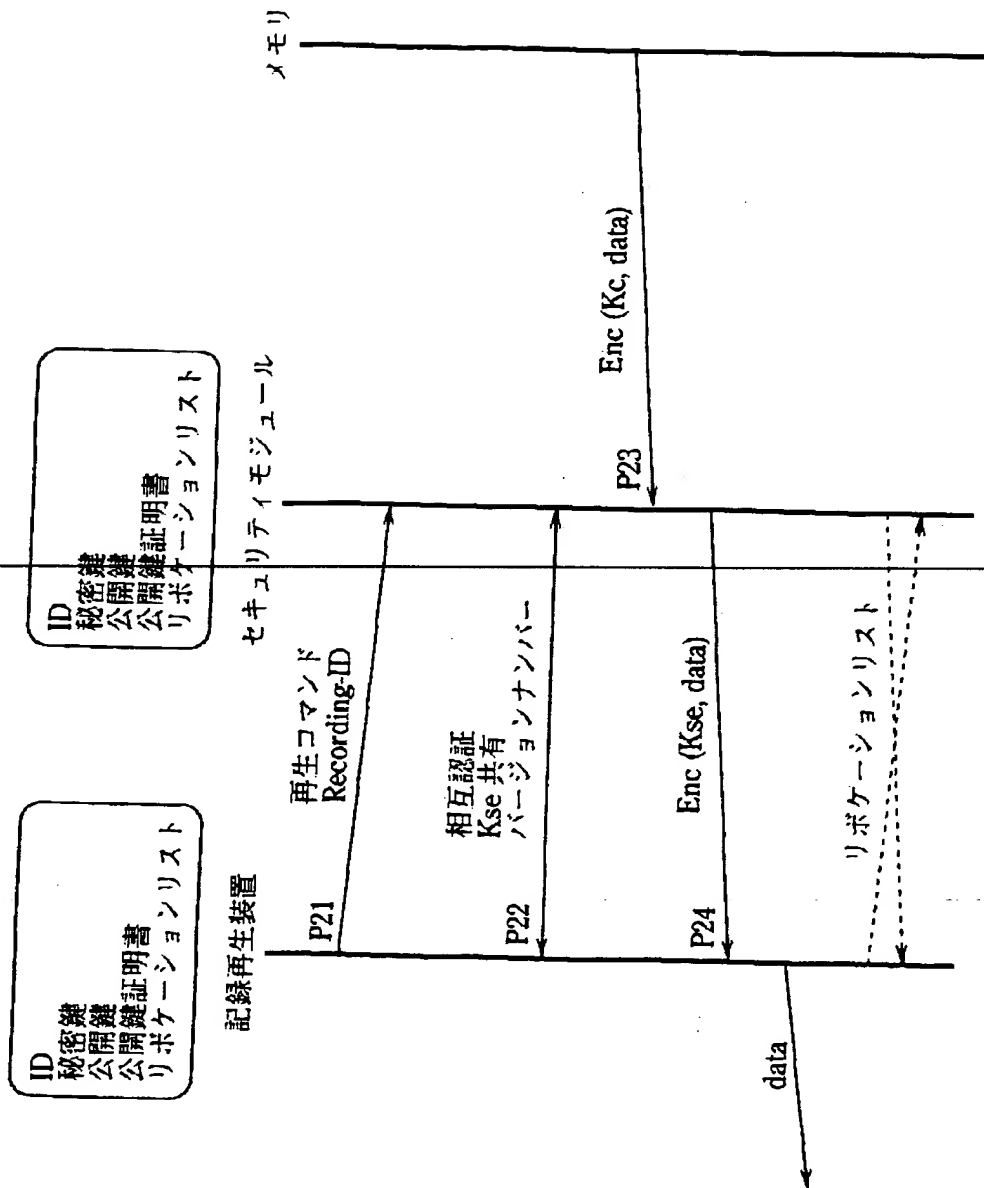
【図 1 1】



【図 1 2】



【図 1 3】



【書類名】 要約書

【要約】

【課題】 映画や音楽などの著作権があるデータの不正な（著作権者の意に反する）複製を防ぐことができるようする。

【解決手段】

光ディスク情報記録媒体 1 0 にセキュリティモジュール 1 3 を持たせ、光ディスク上に記録されるデータを個々のデータごとに異なる暗号鍵で暗号化し、暗号鍵をセキュリティモジュール 1 3 が安全に保管する。また、セキュリティモジュール 1 3 は記録／再生装置と公開鍵暗号技術を用いた相互認証を行い、相手が正当なライセンスを受けた装置であることを確認した上で、暗号鍵を装置に対して与えることにより、不正な装置にはデータを漏らさないようにする。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社
